[H.A.S.C. No. 117–8]

DISINFORMATION IN THE GRAY ZONE: OPPORTUNITIES, LIMITATIONS, AND CHALLENGES

HEARING

BEFORE THE

SUBCOMMITTEE ON INTELLIGENCE AND SPECIAL OPERATIONS

OF THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

HEARING HELD
MARCH 16, 2021

U.S. GOVERNMENT PUBLISHING OFFICE
45–429 WASHINGTON : 2021

SUBCOMMITTEE ON INTELLIGENCE AND SPECIAL OPERATIONS

RUBEN GALLEGO, Arizona, *Chairman*

RICK LARSEN, Washington
JIM COOPER, Tennessee
WILLIAM R. KEATING, Massachusetts
FILEMON VELA, Texas
MIKIE SHERRILL, New Jersey
JIMMY PANETTA, California
STEPHANIE N. MURPHY, Florida, *Vice Chair*
TRENT KELLY, Mississippi
AUSTIN SCOTT, Georgia
SAM GRAVES, Missouri
DON BACON, Nebraska
LIZ CHENEY, Wyoming
MICHAEL WALTZ, Florida
C. SCOTT FRANKLIN, Florida

SHANNON GREEN, *Professional Staff Member*
PATRICK NEVINS, *Professional Staff Member*
ZACH TAYLOR, *Clerk*

CONTENTS

DISINFORMATION IN THE GRAY ZONE: OPPORTUNITIES, LIMITATIONS, AND CHALLENGES

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
SUBCOMMITTEE ON INTELLIGENCE AND SPECIAL OPERATIONS,
Washington, DC, Tuesday, March 16, 2021.

The subcommittee met, pursuant to call, at 11:01 a.m., in room 2118, Rayburn House Office Building, Hon. Ruben Gallego (chairman of the subcommittee) presiding.

OPENING STATEMENT OF HON. RUBEN GALLEGO, A REPRESENTATIVE FROM ARIZONA, CHAIRMAN, SUBCOMMITTEE ON INTELLIGENCE AND SPECIAL OPERATIONS

Mr. GALLEGO. Thank you, everyone, for joining us. Please take a seat.

Before I get going, I have to do some Webex instructions per House and admin. Here we go.

Members who are joining remotely must be visible on screen for the purposes of identity verification, to establish and maintain a quorum, participate in the proceedings, and voting. Those members must continue to use the software platform video function while in attendance unless they experience connectivity issues or other technical problems that render them unable to participate on camera. If a member experiences technical difficulty, they should contact the committee staff for assistance. A video of members' participation will be broadcast in the room and via the telephone/television/internet feed.

Members who are remote must seek recognition verbally and they are asked to mute their microphones when they are not speaking. Members who are participating remotely are reminded to keep their software platform video function on the entire time they attend the proceeding. Members may leave and rejoin the proceeding. If members depart for a short while for reasons other than joining a different proceeding, they should leave the video function on. If members will be absent for a significant period or depart to join a different proceeding, they should exit the software platform entirely and, then rejoin it if they return. Members may use the software platform chat feature to communicate with staff regarding technical or logistical support issues only.

Finally, I have designated a committee staff member, if necessary, to mute unrecognized members' microphones to cancel any inadvertent background noise that may disrupt the proceeding.

Good morning. I call to order this first hearing of the Intelligence and Special Operations Subcommittee on "Disinformation in the Gray Zone: Opportunities, Limitations, and Challenges."

We are seeing unprecedented threats to our democracy and a disturbing rise of authoritarian actors. Anti-democratic forces have capitalized on the rapidly evolving information environment to spread disinformation and misinformation, and exploit fissures in our society. The only way to reverse these trends is through a whole-of-society approach working with partners and allies who share our values.

After two decades of war fighting terrorists in Afghanistan, Iraq, and elsewhere around the Middle East and Africa, we have discovered an even greater threat inside the wire. Gone are the days when we could solely rely on the Armed Forces to fight our wars beyond our borders. The threats and attacks are now here. On American soil. And at home.

The 2018 National Defense Strategy stated that the "homeland is no longer a sanctuary." Our adversaries' use of information and technology has proven that out. They craft and feed misinformation to our news outlets and social media about the safety of vaccines, for example, the efficacy of our institutions, and the depth of our differences, and then they weaponize our own reactions to that misinformation.

So, we have a problem. So much so that last year nine—I repeat, nine—combatant commanders co-sent a letter to the Director of National Intelligence requesting immediate help to combat the pervasive and damaging influence by China and Russia. I want to hear what we are doing to help our commanders. How are we making sure that information about the malign activity of Russia and China is not overclassified, and how are you synchronizing with the State Department and with partners and allies to combat these threats?

Information operations is one way that the United States can protect itself and its partners against dis- and mis-information efforts by China and Russia. We should aspire for cohesion and breadth. We must develop a comprehensive influence strategy to truly protect our borders, our allies, and our interests.

In that context, I look forward to hearing from our witnesses about the Department's efforts to support and build a whole-of-government construct. I want to introduce the three witnesses who will tell us a little about that.

Mr. Christopher Maier, Acting Assistant Director of Defense for Special Operations and Low-Intensity Conflict; Mr. Neill Tipton, Director of Defense Intelligence, Collections and Special Programs; and Mr. James Sullivan, Defense Intelligence Officer.

Following this discussion, we will continue in a closed, classified session.

[The prepared statement of Mr. Gallego can be found in the Appendix on page 25.]

Mr. GALLEGO. I understand that Ranking Member Kelly is on his way from the airport. So, we will get started with our opening statements from our witnesses, and once we are done with our witness statements, we will swing back to Ranking Member Kelly for his opening statement.

And with that, let's start with Mr. Maier. Thank you.

Mr. MAIER. Chairman, we are actually going to start with an intel brief, if that is okay, quickly, and then, shift from there.

Mr. GALLEGO. Go ahead.

STATEMENT OF JAMES SULLIVAN, DEFENSE INTELLIGENCE OFFICER FOR CYBER, DEFENSE INTELLIGENCE AGENCY

Mr. SULLIVAN. Mr. Chairman, Members, good morning. My name is Jim Sullivan, Defense Intelligence Officer for Cyber. Thank you for the invitation to come down here. I will provide you some background on——

Mr. GALLEGO. Mr. Sullivan, please put the microphone closer to your mouth. Thank you.

Mr. SULLIVAN. Thank you, sir.

I am here to provide the threat landscape of our two main rivals, Russia and China, in the information sphere. I will cover more specifics in the closed session.

I will begin with Russia. Russia sees the information sphere as a key domain for modern military conflict. Russia has prioritized the development of forces and means for information confrontation in a holistic concept for ensuring information superiority since at least the 1920s. Russia wages this struggle for information dominance during peacetime and armed conflict with equal intensity using combined electronic and kinetic means and methods through information-technical, information-psychological, and active measures. The Russian government claims NATO [North Atlantic Treaty Organization] countries, led by the United States, have created a powerful information operations system and are expanding and improving it.

Russia sees the information domain differently than the United States and its allies and partners. Russian publications and actions indicate its government maintains a holistic concept of information confrontation. Specifically, information confrontation seeks to dominate the information domain through a combination of what it defines as information-technical effects—or means which seek to manipulate networks, computers, and data—and information-psychological effects, all intended to target people or a population to influence behavior or opinions. We are increasingly seeing the integrated use of cyber-enabled psychological actions, distributed denial-of-service attacks, propaganda disseminated through social media and bots, strategic deception and disinformation, and electromagnetic warfare to achieve strategic goals.

China seeks to influence domestic, foreign, and multilateral political establishments and public opinion to accept China's narratives and to remove obstacles that prevent China from attaining its goals, including the sustainment of the Communist Party regime. The People's Liberation Army [PLA] has developed the concept of "Three Warfares"—which is to say, public opinion, legal, and psychological warfare—as key components of its psychological-cognitive warfare efforts. These efforts are designed to demoralize adversaries and to influence foreign and domestic public opinion.

Similar to Russia, China also takes a broad approach, to include the establishment of cultural centers, taking control of Chinese language print media, and the employment of cyber techniques. China views the cyber domain, in particular, as an ideal platform for strategic influence and deception and disinformation operations. The PLA likely seeks to use digital influence activities to support its

overall "Three Warfares" concept and to undermine an adversary's social cohesion, economy, morale, and governance. These operations are conducted with intensity in peacetime, and we anticipate they would be conducted with increased intensity during armed conflict. The PLA goals for social media influence activities fall into three broad categories: to promote a narrative favorable to China, undermine adversary resolve and social cohesion, and shape foreign governments' policies in favor of China's core interests.

Sir, that concludes my opening statement.

Mr. GALLEGO. Thank you, Mr. Sullivan.

And, Mr. Maier.

STATEMENT OF CHRISTOPHER MAIER, ACTING ASSISTANT SECRETARY OF DEFENSE, SPECIAL OPERATIONS AND LOW–INTENSITY CONFLICT, U.S. DEPARTMENT OF DEFENSE

Mr. MAIER. Thank you, Chairman. Chairman Gallego, Ranking Member Kelly, and distinguished committee members, it is an honor to be with you here today.

As is already stated, I am Chris Maier. I am the Acting Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict. In this capacity, I serve as the principal civilian adviser to the Secretary of Defense on special operations and low-intensity conflict matters, including the employment of special operations forces. On behalf of the Under Secretary of Defense for Policy, I also provide oversight for information operations.

Building on the brief laydown on the threat you received just now from the Defense Intelligence Agency, I am here with my colleagues from the Department of Defense to discuss our approach to adversary disinformation in the gray zone and the Department's efforts to gain and maintain the operational advantage in this evolving threat environment.

Adversary use of disinformation, misinformation, and propaganda poses one of today's greatest challenges to the United States, not just to the Department of Defense. Russia and China, as well as non-state actors, understand that in today's information environment they have real-time access to a global audience. With first-mover advantage and by flooding the information environment with deliberately manipulated information—that is, mostly truthful with carefully crafted deceptive elements—these actors can gain leverage to threaten our interests.

Although we are here today to discuss various DOD [Department of Defense] efforts, we recognize that we do not have a monopoly on U.S. Government capabilities to combat disinformation, nor should we. The Department of Defense is one of a whole-of-government approach to this challenge, and other civilian departments and agencies have critical roles and responsibilities which demand close interagency coordination and clear authorities. Coordinated interagency effects can complement the efforts of each department and agency to defend the Nation against disinformation and to reach and engage global audiences.

As we strive to leverage DOD's information operations capabilities in competition with malign actors, we must first acknowledge, as reiterated in the recently published Interim National Security Strategic Guidance, that we will actively support elevating diplo-

macy as our tool of first resort. DOD directly supports the Department of State's Public Diplomacy teams and the Global Engagement Center, and complements the activities of the U.S. Agency for Global Media.

Within DOD, we organize our efforts to combat disinformation, misinformation, and propaganda in four broad lines of effort, all supported by a foundation of intelligence support, interagency collaboration, and partnerships. These four areas are: countering propaganda by adversaries, force protection, countering disinformation and strategic deception abroad by adversaries, and deterring and disrupting adversarial malign influence capabilities. I will briefly touch on each one of these efforts.

Countering propaganda. Propaganda, especially with a capable sponsor spreading it to susceptible audiences, can often drown out truthful information and create barriers to fact-based messaging. Public Affairs is the lead within DOD for countering propaganda that affects U.S. military objectives. Public Affairs also leads the Department's efforts to inform domestic and foreign audiences of adversaries' attempts to manipulate behavior in this domain. Other DOD capabilities support Public Affairs' effort to lead proactively with truthful, verifiable, fact-based messaging. DOD efforts to engage foreign audiences overseas support the Department of State's lead to inform foreign audiences.

Next, force protection. Our soldiers, sailors, Marines, airmen, guardians, civilians, and their families are part of the American public directly targeted by malign actors' disinformation, misinformation, and propaganda. DOD views this as a critical force protection issue. The military services are proactive in building resilience against these threats. Enabling the force to recognize deceptive information tactics by adversaries' information operations, developing digital literacy, and employing critical thinking skills are a few key initiatives within the force protection line of effort.

Third, countering disinformation abroad. At DOD, we also draw upon operational and informational capabilities, such as Military Information Support Operations, often better known by its acronym MISO, to generate narratives to compete against disinformation efforts directed at foreign audiences. These DOD capabilities can amplify and complement existing themes and messages to inform audiences that cannot be reached through traditional communications channels. To counter disinformation abroad, at DOD, we pursue a comprehensive and deliberate approach, working in close consultation again with State, to connect with audiences globally in real time to build communications that foreign audiences trust. Knowledge and trust by foreign audiences will reduce, and even suppress, the impact of malign influence activities.

And then, finally, deterring and disrupting adversarial malign influence capabilities. Perhaps DOD's greatest strength lies in our ability to align narratives with actions in the domains of land, sea, air, cyber, and space, and information-related capabilities against key weaknesses in the adversaries' information environment. Further, as we continue to seek to empower and work through partners, DOD draws on our knowledge, skills, and infrastructure to enable allies, partners, proxies, and surrogates to compete with malign actors, often near-peer competitors in the information envi-

ronment, and for the benefit of their own populations, as well as our own. Our partners are force multipliers in deterring and disrupting adversarial disinformation.

Through our ability to match words with deeds, we complement the efforts of our diplomats to deter malign behaviors, incentivize cooperation, and at times compel action. DOD's ongoing efforts to defend forward, to actively detect, assess, and, when directed, disrupt adversaries' disinformation, misinformation, and propaganda, bolsters our actions in the information environment.

My colleague, Neill Tipton, Director of Defense Information, will speak in just a moment about intelligence support to these efforts. To foreshadow from policy and operational perspectives, intelligence support is essential to the whole-of-government partnerships that are key to our collective U.S. Government success against adversary disinformation, misinformation, and propaganda. And to reinforce once again, our international allies and partners are essential in reinforcing our collective efforts, often by contributing unique capabilities to countering adversaries' malign efforts. We are most effective when bolstered by their perspectives and their integration into our planning and execution.

In sum, the Department continues to invest in our capabilities and capacities, so that we are best positioned to mitigate and defeat the disinformation efforts of our adversaries. We continuously aim to improve our speed, agility, efficiency, and effectiveness, and, most importantly, teamwork across the U.S. Government and internationally.

We appreciate this subcommittee's attention to this critically important issue and your ongoing support to the Department's efforts in this information domain. Thank you for the opportunity to be here today.

I will now turn it over to my colleague, Neill Tipton, who will address how intelligence supports these efforts. After that, we look forward to answering your questions.

Mr. GALLEGO. Thank you, Mr. Maier.

Mr. Tipton.

STATEMENT OF NEILL TIPTON, DIRECTOR OF INTELLIGENCE FOR COLLECTIONS AND SPECIAL PROGRAMS, U.S. DEPARTMENT OF DEFENSE

Mr. TIPTON. Chairman Gallego, Ranking Member Kelly, and distinguished committee members, thank you for the opportunity to be here today.

So, as previously mentioned, I am Neill Tipton, Director for Defense Intelligence for Collection and Special Programs in the Office of the Under Secretary of Defense for Intelligence and Security.

Today, I will speak to you about the intel support needed to ensure that the Department maintains the upper hand against the challenge of disinformation in the gray zone. I will focus my remarks today really on four key areas where we are prioritizing intel support to the various efforts we are discussing: partnerships in intel support; intelligence support to irregular warfare; intelligence support to operations in the information environment; and support to combatant commands, which gets at Chairman Gallego's comments about the colloquially known 36-star memo.

I will start with partnerships in intelligence support. So, underpinning all these efforts is a strong commitment to a whole-of-government partnership and decision cycle that constantly assesses the effects of misinformation and propaganda, and seeks to attribute these efforts to the responsible parties. This requires active cooperation across the responsible departments and agencies, as well as direct support from the intelligence community. The DOD leverages its information capabilities to gain and maintain the information advantage and integrates with the tools of other departments as part of a broader and more comprehensive approach. Our international allies and partners——

Mr. GALLEGO. Mr. Tipton, can you slow down a little?

Mr. TIPTON. Absolutely.

Mr. GALLEGO. I don't have you on the clock. So, you are good to go.

Mr. TIPTON. Okay.

Mr. GALLEGO. Thank you.

Mr. TIPTON. I can do that. Thank you.

Mr. GALLEGO. Yes, it may be that I am just a slow learner more than anything else.

Mr. TIPTON. Okay. Our international allies and partners also bring reinforcing and often unique capabilities in our endeavors to counter adversaries' malign efforts, and their capabilities will be integrated into our planning efforts as well.

The recently signed Defense Intelligence Strategy prioritizes China and Russia. The strategy calls out a specific action to prioritize intelligence support to strategic competition and influence efforts. The Defense Intelligence Enterprise will help advance U.S. influence and counter-coercive campaigns via robust and focused intelligence support to sensitive and special activities, influence, deception, and, more broadly speaking, operations in the information environment.

We would like to highlight for the committee three specific examples of ongoing actions that OUSDI&S [Office of the Under Secretary of Defense for Intelligence and Security] is supporting through our role within DOD and our partnership with the broader intelligence community. So, those are, as mentioned, intel support to irregular warfare, intelligence support to operations in the information environment, and intelligence dissemination to support combatant command messaging and counteractivities.

So, intel support to irregular warfare. In support of the Irregular Warfare Annex to the 2018 NDS [National Defense Strategy], OUSDI&S, in partnership with the Joint Staff J–2, is supporting specific lines of effort to enable DOD to improve understanding in what we all the multi-domain environment. The several lines of efforts focus on identifying indicators and warnings, integrating collection, leveraging big data, reinforcing intelligence-sharing best practices, and assessing all the policies and processes that support these efforts.

Intelligence support to operations in the information environment. As I am sure you are aware, my colleague, Mr. Maier, has oversight for operations in the information environment. We have established, as part of that, a Defense Intelligence Support to Operations in the Information Environment Working Group that has got

a variety of activities underway to increase and enhance that support, one of which is a new effort, working with ODNI [Office of the Director of National Intelligence], to focus the national intelligence community on collection efforts on assisting us in the conduct of influence-related activities against key adversaries. That work is still ongoing.

Also, that group is focused on drafting and staffing a new DOD instruction for intelligence support to operations in the information environment that would codify recommendations that came out of a 2019 JROC memo—so the Joint Requirements Oversight Council—that provided some specific recommendations to the Department on how we enhance these activities. Amongst other things, it will direct the DIE [Defense Intelligence Enterprise] to prioritize resources for intelligence support to OIE [operations in the information environment] in the next published Consolidated Intelligence Guidance and will help us shape and work, again, as I mentioned, with the DNI and the national intelligence focus groups to drive some of these key concepts into the broader prioritization framework that the DNI [Director of National Intelligence] manages for the IC [intelligence community].

And finally, I will talk about combatant command support. Another line of effort, as you had mentioned, for which we are providing intelligence support to OIE has been through the joint DOD-Director of National Intelligence response to the intel demands from the combatant commands. As you mentioned, in January of 2020, nine combatant commanders signed that memo out—we referred to as the 36-star memo—which asked for increased support from the IC for messaging and countering disinformation operations, as part of great power competition.

In response, we partnered in an ongoing effort to streamline processes for downgrading, declassifying, and disclosing intelligence in support of operations in the information environment. We look to complete the current efforts in response to that memo by September of this year, while continuing follow-on initiatives to increase the use of open-source intelligence and to determine policy and resourcing strategies to provide the most effective intel support to OIE going forward. And then, finally, we are working across the Department to improve our training of intelligence personnel in this space and to optimize our tradecraft as appropriate to support operations in the information environment.

So, the DIE will continue to support these efforts and ensure the Department is postured for success in this area. We appreciate your attention to this very important matter. This concludes my remarks, and I look forward to your questions. Thank you.

[The joint prepared statement of Mr. Maier, Mr. Tipton, and Mr. Sullivan can be found in the Appendix on page 27.]

Mr. GALLEGO. Thank you, Mr. Tipton.

I recognize Member Kelly for an opening statement.

STATEMENT OF HON. TRENT KELLY, A REPRESENTATIVE FROM MISSISSIPPI, RANKING MEMBER, SUBCOMMITTEE ON INTELLIGENCE AND SPECIAL OPERATIONS

Mr. KELLY. I apologize to you guys for being late. I literally came straight off a plane straight here. So, thank you for being here and I thank you for being patient.

Mr. Chairman, thank you for your opening remarks and your leadership in organizing this morning's important hearing.

Today, we will hear from three professionals in our Intelligence and Special Operations Subcommittee for both an unclassified and classified conversation about the spread of disinformation from our adversaries. To highlight just how seriously we take this disinformation, Chairman Gallego has chosen it as the subject of the first official hearing of the new Intelligence and Special Operations Subcommittee.

The subcommittee was recently briefed on the threatening activities of China. Just last week during a full committee hearing, we heard from Admiral Phil Davidson, Commander, INDOPACOM [Indo-Pacific Command]. He described ways the Communist Party of China uses a whole-of-government approach to exert control over the regions.

One of the ways China conducts this external aggression and coercion is via the perverse spread of disinformation. This is most clearly seen in China's information campaigns around the coronavirus pandemic. The spread of malign information has sought to spread panic and distrust within the U.S., and even alleged that the United States Army was responsible for bringing the virus to China.

China is not alone in these efforts. State-backed accounts in Russia and Iran also constructed manipulative narratives about our vaccine efforts. In fact, Russia has repeatedly used the gray zone to spread disinformation. An article in The Wall Street Journal from March 7th describes activities of Russia's intelligence enterprise across multiple state-backed, online news sites. The article outlines specific actions taken to spread misleading and false narratives to discredit the efficacy of the Pfizer vaccine.

The use of disinformation is not just linked to the current pandemic, however. Our adversaries have long used this gray zone to operate, push false narratives, and undermine the national security interests of the United States. A memo signed last year by nine combatant commanders drives home just how important this issue is. Recognizing the need for increased support from the intelligence community to combat this threat, they note, "malicious efforts by Russia and China across the information domain to seed discontent, weaken trust, and undermine alliances." The threat is real and growing.

I am interested to hear our witnesses' views on how to best train and equip our intelligence professionals to counter this threat. I want to thank our witnesses in advance for their time today. I look forward to continuing work with our intel and special operations professionals during the 117th Congress.

Mr. Chairman, I yield back.

Mr. GALLEGO. Thank you, Ranking Member Kelly.

We will now go to questions. And again, for our members, we will be limiting it to 5 minutes. And when you are recognized, please make sure to unmute your microphone. And we will begin with me.

Countering misinformation, while an important DOD function, also involves the State Department and intel [community]. How will ASD SO/LIC [Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict] and the Under Secretary of Defense for Intelligence work across the defense intelligence communities to ensure coordination of effort in this space? We will start with you, Mr. Maier.

Mr. MAIER. Thanks, Mr. Chairman.

So, I think, in the first instance, it is important for us to clearly articulate to our intelligence community colleagues the requirements. And there is a wide definition of what we do in the information operations space and there is a limited number of intelligence resources. So, it is really incumbent on us on the policy side, especially from the oversight perspective, to make sure that we are communicating clearly what those priorities are for intelligence support. Everybody needs intelligence in this day and age to do everything. And so, I think it is incumbent on us to really be clear in working with the intelligence community, beyond just the Department of Defense, what those requirements are.

I imagine my colleague would be able to speak to the intelligence requirements piece and how he manages those.

Mr. TIPTON. So, Chairman, just a couple of thoughts. One is nothing we do is done in a vacuum, and USDI ensures we work in a very tight partnership with ODI.

Mr. GALLEGO. Mr. Tipton, please bring the microphone closer to you.

Mr. TIPTON. Sorry. So, I would comment, first, by saying that nothing we do is executed in a vacuum. We work very closely with the Office of the DNI on all these kinds of activities. And this is a specific case where we are partnered very tightly with them as we respond to the 36-star memo and other kinds of activities that are necessary to operate in the information environment.

And the same goes with our allies. We recognize that we have to operate as part of a greater whole, and we are very tightly lashed up, especially with our closest allies, as we develop new products, reshape the priorities, develop all the supporting processes and enabling activities that we have to design and implement in order to reshape the outputs of the intel enterprise, which for 20 years has been focused on other problem sets, to how do we refocus on this problem set and support customers like ASD [Assistant Secretary of Defense] Maier and other operators in this space.

Thank you.

Mr. GALLEGO. Thank you. I appreciate the necessity of activities conducted by the Department to mitigate or curtail nefarious actions by our adversaries' intent to undermine and counter the strength of our military. However, information operations are one small part of what should be a larger, whole-of-government approach to combat malicious Russian or Chinese behavior. Some of our allies and partners already do this, but they are much smaller

than us and their problems and opportunities are different from ours.

Given the proliferation of disinformation, misinformation, and propaganda, would it be appropriate to call for a whole-of-government influence campaign and strategy to ensure nested and synchronized efforts to the benefit of our national security objectives? And to follow up with that—well, Mr. Maier, if you wanted to start with that?

Mr. MAIER. Mr. Chairman, yes, I think it is, and I think we endeavor to do so in a number of focused efforts. Obviously, China and Russia use, and Iran and other non-state actors use, this technique across the whole range of different issues. So, we need to be precise as we leverage those interagency efforts and with our partners.

Mr. GALLEGO. And so, we recognize that we need to do it, but trying to bring together different departments, different agencies, with different goals, different missions, to be focused requires at least someone to be a coordinator of that. Who is coordinating that at this point?

Mr. MAIER. Mr. Chairman, we would look to the National Security Council [NSC] staff to lead those interagency efforts, but the Department of Defense and State already organically work together on a number of these. But the real quarterback in this system of the interagency is going to be the NSC staff, sir.

Mr. GALLEGO. Yes. Mr. Maier, what role does the ASD SO/LIC play in information operations, specifically, the interplay of big DOD, SOCOM [Special Operations Command], and the interagency?

Mr. MAIER. Mr. Chairman, I would answer your question in two ways. First, as has been directed by [section] 922 in the NDAA [National Defense Authorization Act] from 2017, it reinforces the role that ASD SO/LIC plays as the service-secretary-like or administrative chain of command. So, we have responsibility/civilian oversight for ensuring the force is equipped to do these operations, SOCOM, but also the components—USASOC [U.S. Army Special Operations Command], Navy SEALs [Sea, Air and Land teams], Air Force Special Operations Command, a whole series of others.

And then, on the policy side of things, we are the direct support to the Under Secretary for Policy for integrating information operations and these types of disciplines into the policy development process for the Department of Defense.

Mr. GALLEGO. Thank you.

Representative Kelly.

Mr. KELLY. Mr. Chairman, I yield to Mr. Bacon, who is prepared to move forward with questions.

Mr. BACON. Thank you, gentlemen, for sharing your expertise. We sure appreciate it.

One of the things that I have noted, that our adversaries often use our partisan political scenes for disinformation, which makes it harder for us to counter. How do we overcome that when, say, Russia in 2016 uses disinformation in a way that makes it hard in a partisan environment to counter? I would be curious for your thoughts on that. Thank you.

Mr. GALLEGO. Mr. Maier, is that a deepfake that we just saw with the two Bacons?

Mr. MAIER. I am not sure, Mr. Chairman.

Mr. GALLEGO. All right. Okay, Mr. Bacon. Sorry.

Mr. BACON. Could you hear me all right? I asked the question.

Mr. MAIER. So, I will take that broadly, and then, defer to the intel community on the specifics of this. But I think it is a well-recognized technique that these malign actors are using, and I think some of this is, again, some of the points I made in building resilience and ensuring that what is coming out, at least from the U.S. Government's information sources, whether it is Public Affairs or others, is truthful information.

As to how we best counter adversaries exploiting that, I will defer to my intelligence colleague for how they are doing that.

Mr. SULLIVAN. Yes, Mr. Bacon, Jim Sullivan from DIA [Defense Intelligence Agency].

So, it really does begin with making sure that we are working across the spectrum of DIA, NGA [National Geospatial-Intelligence Agency], NSA [National Security Agency], CIA [Central Intelligence Agency], FBI [Federal Bureau of Investigation], and others, and enhancing our own capability inside the Defense Intelligence Enterprise to, number one, understand who the cyber actors are; what publications, what social media platforms are they using; what is their strategy/doctrine/intent at getting to the American public, and what specifically is it that they are targeting. Once we have the bubble on that, then we can work with others inside the combatant command, other intel agencies, and be better equipped to counteract that.

Mr. BACON. One thing that I saw in France, I thought they did a good job to say right upfront, candidly, this is what Russia is doing and they are trying to play on partisan divides. And I just think we have to be more candid with our voters and with our citizens when this happens.

One other question for you before I yield. DOD's 2020 China military power report identified how China uses its so-called "50 Cent Army" to, among other things, try to influence public opinion towards the pro-China perspectives. They noted how, in 2019, Facebook and Twitter had deleted some accounts spreading disinformation regarding the protests in Hong Kong. So, over the past year, have social media companies been more effective at reducing the spread of disinformation, especially from China and Russia? Thank you.

Mr. SULLIVAN. Yes, I will go ahead and take that, Mr. Bacon. So, I think, in the last several years, social media, and also, too, commercial vendors, have operated quite prolifically in this space and have gotten very, very capable, both in determining/attributing where this activity is coming from, and then, being able to use algorithms in order to delete accounts.

Now I can't speak to what they are doing for China at this moment, but the trend is I think moving in a positive direction. When you take that in combination with what we are doing in open source, I think we are getting a better handle on at least false narratives, again, identification of the media platforms that they are

using. And I think, as time goes on, we are better postured to do that.

Two years ago, I think it was quite difficult to be able to understand what was a false account. But the tradecraft has gotten much better; being able to identify it has gotten much better. And I have every expectation that in the future that is only going to improve.

Mr. BACON. I will just close with two comments. First, we have a long history in our country of being successful in this area. In World War II, multiple examples where we can overcome. So, we have it within our ability to win in this spectrum.

And I will just close, also, by saying thank you to each of you for serving and defending our country, and I appreciate what you do every day. With that, I yield back.

Mr. GALLEGO. Thank you, Representative Bacon. Thank you, Member Kelly.

I now recognize Representative Larsen.

Mr. LARSEN. Thank you, Mr. Chair.

Mr. Maier, given what we have heard today with regards to SOCOM, does it—this is sort of a loaded question—but does it imply a need for changing either who we recruit, the skills they have, the skills we develop in SOCOM, and the structure of the teams within SOCOM, in order to address these particular challenges? Have you thought through that and can you give us some idea of what you are thinking?

Mr. MAIER. Yes, thanks, Congressman Larsen. That is, I think, a very important question.

And I have the benefit in the role I play to support the Secretary of Defense, who has made diversity one of his number one challenges. I had the benefit of sitting in on a conversation he had with General Clarke, the SOCOM commander, and he made that abundantly clear, that diversity is an operational imperative. It has the benefits that you articulated in your question of being able to bring different perspectives, different ways of communicating, knowledge of culture—things that, if everybody looks the same, if everybody thinks the same, are going to render us not particularly effective in these challenging environments.

We are evolving, I think, as a country and a force from heavy focus on the counter-VEO, violent extremist organizations, to a much more diverse threat environment where information is one of the tools they are using. And we have got to be able to play their game against them and beat them in some respects on their own playing field. That means the ability to speak languages, the ability to draw on cultural innuendos that aren't necessarily obvious to those that may have been trained for other purposes.

Mr. LARSEN. So, within SOCOM, do you think they are evolving fast enough to support this?

Mr. MAIER. I think, sir, that they would say they are not evolving fast enough. As you know, in training special operations forces, it really requires recruitment and training far down the line, very early in the process. And that is something that all the components, whether it is the SEALs, the Air Force Special Operations components, or the Army components, Marine Corps, are looking at

how they get farther downstream in their recruiting in order to do what you are articulating.

Mr. LARSEN. As Acting ASD SO/LIC, do you think you have enough authority, and would you have enough authority as a permanent confirmation, to push that along?

Mr. MAIER. At this point, I think I do, sir. But a lot of this is going to be just persisting, keeping on this. This is a priority that is going to take, unfortunately, a long time to actually see fruition, and we are going to have to stay on this. It is a strong partnership, I think, with SOCOM and they recognize this need and have prioritized it as well. That is the best arrangement, I think, regardless of bureaucratic standing, to get to a success.

Mr. LARSEN. And on bureaucratic standing, I understand that SECDEF, or the Secretary of Defense, is reviewing the changes that former Secretary of Defense Miller put in place about the role of ASD SO/LIC. Do you have any insight for where that is now? My personal view is that, regardless of the outcome, we need to have a stronger civilian oversight over SOCOM forces.

Mr. MAIER. Congressman, thank you for that statement. It is a decision that is before the Secretary of Defense now. I think the options are fairly obvious. They are: do we keep it the way it is with SO/LIC separate from all the other entities in the Department or do we integrate it into policy pieces? But I don't think there have been any options discussed in which ASD SO/LIC does not—and I reiterate that, does not—continue to report to the Secretary of Defense as a principal staff assistant for that administrative piece of oversight and civilian oversight of Special Operations Command, sir.

Mr. LARSEN. Thanks. I just don't want any confusion about the letter that was sent a few weeks ago from members of the subcommittee and others about the intent of the letter.

Back to sort of the broader—I have got 56 seconds left—back to the broader issue of intelligence and intelligence sharing. I am going to have to get caught up a little bit more on all the letters. I mean, I understand all the lettered agencies you talked about. And perhaps you can think about this for the classified: if you think there are any gaps in how that information gets communicated within the DOD and between agencies, so that it can be most effectively used. I don't know if there is something you can say about that now. Mr. Tipton, you look like you are eager to answer that.

Mr. TIPTON. Yes, Congressman, I will just comment that we are rebuilding muscle memory that we haven't exercised really since the Cold War, as we operate in this kind of information domain. And so, clearly, there are gaps in how we do that and we are working through that. We can talk a little bit more about that in the closed session.

Mr. LARSEN. I look forward to it. That is fine.

And I yield back, Mr. Chairman. Thank you.

Mr. GALLEGO. Thank you, Representative Larsen.

Representative Scott.

Mr. SCOTT. Thank you, Chairman. I don't have a whole lot. I will say that I was on one of our military installations the other day and speaking about kind of the width and the depth of the anger

that I see out there. And one of the generals suggested to me that they were seeing it in their ranks, too, and that I should watch the documentary "The Social Dilemma," and how people are able to use information against us.

And so, just a suggestion for the committee, and maybe looking for comment from the people that are presenting, is: are we discussing with our soldiers the potential for the use of disinformation and misinformation through social media to create bias in the ranks or dissent in the ranks of the military? Do you know if we are actually having discussions with our troops on that?

Mr. MAIER. Mr. Scott, I can answer that question. So, absolutely, and one of the main pillars that I mentioned in my remarks, and that I can go into a little bit more depth on, is the force protection concerns associated with intentional misinformation and disinformation through social media.

A critical component of what Secretary of Defense Austin is looking at, too, is extremism. And a key component of these standdowns that we are all involved in, not just the uniformed side, but the civilian side, is looking at the influences from the outside that do contribute to extremism and, as one of your colleagues said, attempts to divide not only the forces, but us, as citizens.

And I think we look at this through the lens of every soldier is both a citizen and a member of the Armed Forces, and having to look at both those perspectives is a critical piece as they are looking at social media, and we look to, as much as possible, make them resilient against what we know are concerted efforts to attempt to divide and in some cases drive them to extremism.

Mr. SCOTT. Well, I would finish with this: one is I think it has been very effective, what they are doing, unfortunately. And as this current generation comes out of high school and college, the first generation where, basically, everything they have done has been on the internet, I think we need to expand beyond the scope of the military as fast as we can in advising the American citizens what is happening with the ability of outside influences who do not like our country to influence our attitudes towards each other in this country and how damaging it is to us.

With that, Mr. Chairman, I will yield.

Mr. GALLEGO. Thank you, Representative Scott.

Representative Keating. Representative Keating.

Mr. KEATING. Thank you, Mr. Chairman. I heard my name.

I just want to thank the witnesses. This is an important issue, and I am just pleased that, just more commentary, I am pleased that the new Secretary of Defense is taking these issues as seriously as he is. And we all have to work, and I just want to continue to work, particularly in the other committee I am on where we are dealing with some of the malign actors in this field, with Russia and some of their activities.

So, that is all I had to say as a comment going forward. But I thank you.

And thank you for having this as your first full hearing, Mr. Chairman. I think it is an important one. I yield back.

Mr. GALLEGO. Thank you, Representative Keating.

We have Representative Franklin.

Mr. FRANKLIN. Thank you, Mr. Chairman. And thank you, gentlemen, for your time this morning. This is a very critical topic.

I just have a couple of questions for Mr. Maier. In your testimony, you referenced ongoing efforts to detect, assess, and then, when directed, disrupt adversaries' disinformation, misinformation, and propaganda. I am just curious, just for my own edification, what is the trip line for when that takes place? Who is the authority to direct that action? And then, what would a response look like to that misinformation or disinformation?

Mr. MAIER. Yes, sir. So, this is going to be a "it depends" answer a little bit here. And in open forum, what I would say is that a key element of being flexible in the information operations space is ensuring that authorities are delegated down to the appropriate level with the appropriate risk built into that.

And so, I think, if you are talking about activities that, on one extreme, could be kinetic in nature—and that is not outside the realm—those are going to be the purview, of course, of the Secretary of Defense or delegated down. If you are talking about the ability to go out and push back on a narrative, in many respects that is at lower levels within Public Affairs or even within the Military Information Support Operation, generally, in support to the State Department Public Diplomacy and Public Affairs. So, it is going to depend in many respects on what the action envisioned is and how that is viewed from a risk perspective. But the success here is predicated on delegating to the lowest level possible, sir.

Mr. FRANKLIN. Okay. I appreciate that, and that sort of feeds into my next question with regard to an overall strategy for how we would approach this. In section 1239 of the NDAA for Fiscal Year 2020, it called for development of a comprehensive strategy to counter the threat of malign influence by the PRC [People's Republic of China] and Russia. And I think that was due within 6 months, which would have been probably June or so of 2020. Can you tell us where that stands, elaborate on the status of that effort?

Mr. MAIER. Congressman, I am going to have to take that as a request to follow up. I don't know exactly where that is.

Mr. FRANKLIN. Okay. All right then. Thank you, Mr. Chairman. I yield back.

Mr. GALLEGO. Thanks.

Representative Sherrill.

Okay. We will come back to Representative Sherrill. In the meantime, do you have anybody?

Mr. KELLY. No.

Mr. GALLEGO. No? Okay, we will move on to Representative Panetta.

Mr. PANETTA. Thank you, Mr. Chairman. I appreciate this opportunity.

And, of course, thank you to all the witnesses for your service, your preparation, your testimony especially. Thank you very much.

I guess—and correct me if I am wrong—but the 1st Special Forces down at Fort Bragg recently announced an information warfare center just for these types of operations. I guess their main goal is to deliver an "influence artillery round," quote-unquote. Can you give me a little information about the center? Can you give me

a little information about what that influence artillery round would look like?

Mr. MAIER. So, sir, I am going to have to take that for further follow-up to give you an exact answer. But I think it is indicative of what we are trying to do across the force, which is really elevate this issue to a point where I wouldn't want to articulate or even speculate on what they mean by an "information artillery round," but I think that it speaks to the idea that information is a part of our warfighting concept, and therefore, we bring this into the same series of options we would bring, kinetic or other capabilities that might be more traditional, sir.

Mr. PANETTA. Understood. Understood. On that note, do you think or do you know, or can you surmise, if there are plans for other similar types of centers in the future for not just special operations, but other parts of our military?

Mr. MAIER. Yes, sir, I think not only do we envision those, we have got a number of these that are up and operating. The Joint MISO Center down at Special Operations Command is actually an outgrowth of something that Central Command developed. And the realization was we need to be doing this globally. So, that is one that I know this committee has in the past looked into, and we continue to be supportive of it in concept. That is not just because it's at SOCOM, is in a special operations thing; that is all the combatant commands. And so, that brings, we hope, an economy of scale to those efforts.

Mr. PANETTA. Right. Thank you. So, kind of going from looking inward to looking outward, how do you think—you know, Russia, obviously, has kind of set the pace on this, and China has followed. How do you think they are going to evolve with their hybrid warfare going forward and using these types of information/disinformation warfare?

Mr. SULLIVAN. Yes, Congressman, I will take that one, from DIA. So, it has been said in the past that, in the information sphere, that Russia introduces bad weather, whereas China is changing the climate. I would say that that is an accurate statement, except to your point, it is reversed. I think it is Russia that is changing the climate, and I think it is China that is introducing bad weather.

To further complicate it, though, China will grow into that role. China will use technology. China will use machine learning and AI faster than the Russians will do it. Russia is, without question, ahead because they are a lot more prolific and they are a lot more destructive, and they have a slightly different intent, which is they are much more aggressive in terms of trying to undermine U.S. democracy and enhance social—or I am sorry—to degrade social cohesion in the United States. China is not necessarily up to that.

But, to answer your question broadly, the threat in the information domain is here to stay because it really comes down to conventional military overmatch, of which neither country has that against the United States. Cyber is a great equalizer, in that nobody is 100 percent mature in this domain, and information dominance is effective, it is cheap, and it is quick.

Mr. PANETTA. Thank you for that answer. I appreciate that.

Is there one theater, in particular, that each of those near-peers are focusing on? Are they sticking to their areas of influence? Or are you seeing that in other areas, Africa, or so forth?

Mr. SULLIVAN. So, it all depends. It all depends on the actor. Both are global. Russia has a much more massive global presence. They are very much entrenched in Africa, very much so in Eastern Europe. They still try to look at really sort of sowing discord in areas in Europe in which we have a forward presence. China, of course, is very interested in ASEAN [Association of Southeast Asian Nations], in the South Pacific, but it, too, also has a global narrative as well in terms of trying to really present the Chinese Communist Party as an alternative to the United States and Western democracy. I will get more into that in the closed session. But, to Mr. Maier's point, it depends. It really depends on the objective and it depends on the actor.

Mr. PANETTA. Understood.

And then, obviously, this may be something in the closed session, but looking at either our friends or those who are not so friendly to us, are you seeing other nations develop into this area with a little more skill that you wouldn't think coming from them? I mean, either allies, friends, or foes, which ones are we watching when it comes to this type of misinformation in gray zone warfare?

Mr. SULLIVAN. Yes, everybody plays in this sphere to some degree, including us. I don't see an enormous threat from any of our allies or anybody who I would not consider to be China and Russia. Certainly, the DPRK [Democratic People's Republic of Korea] and the Iranians also play in this. And if I had to stratify it, again, I would put Russia as number one, China as number two, Iran as number three, DPRK as number four.

Mr. PANETTA. Understood. Okay. Great. Thank you. Thank you again to everybody.

Mr. Chairman, I yield back. Thank you.

Mr. GALLEGO. Is Representative Sherrill available? One more time, Representative Sherrill?

[No response.]

Mr. GALLEGO. Okay. If there are no more questions, we are going to adjourn for 15 minutes.

And we have one question. Yes, Representative Larsen.

Mr. LARSEN. Yes, this won't be long.

But, for Mr. Maier again, or anyone else, within SOCOM, they have the MISO capability, the responsibility. And that is supposed to be web-based, but there is a lot of non-web-based information operations that occur. So, when we hear from you about SOCOM's responsibility, is it limited to web-based information operations, or how are you sharing across this intelligence domain the totality of information operations? And then, could you help me understand what you all mean by information domain as well? So, it is a real short question, but, like everything, it is always the answer that is long.

Mr. MAIER. Congressman Larsen, yes, sir. So, maybe if it is okay, I will take the last question first, and then, speak to the SOCOM context.

So, I think—not to recite doctrine for information operations, but what we really mean by that is those operations that are in that

operational sphere, informed by the strategic, informed by the tactical, but really that connection between. So, if there is strategic guidance, and we are implementing a strategic approach, the information component of that is really bringing that strategy down to tactical execution. That can be Public Affairs. That can be Military Information Support Operations. That can be a host of other things. And it is really the discipline, as we would look at it doctrinally. What I think this hearing has elicited is it takes on a lot of different forms. I think there is a defensive and offensive component to it. As we think of it from the Department of Defense, we think of it in both contexts.

On your question of Special Operations Command and MISO, they are the proponents, as we use the term, for Military Information Support Operations. My citing the Joint MISO WebOps Center was the entity that they built there to operate in the free-flowing nature of cyberspace for MISO. But SOCOM is supporting the global combatant commands, and the global combatant commands are the ones actually executing MISO operations in the far fletches of the world that we are operating in. So, done so in conjunction with the chiefs of mission approval in the country teams in the particular countries they are operating.

Does that answer your question?

Mr. LARSEN. Maybe we can get into it a little more in the classified. You might help me understand with some examples on that.

Mr. Sullivan, early on, you said Russia sees the information domain differently than the U.S. sees the information domain. Is there an answer you can give us about what those differences are in this setting?

Mr. SULLIVAN. Yes, Mr. Larsen. So, by and large, Russia brings really the full spectrum. Russia does not differentiate information confrontation and disinformation the way we do. They look at it much more holistically than we do. They look at it through the electromagnetic spectrum. They look through active measures. They incorporate it into all aspects of cyber warfare, to include intelligence collection and the like.

We tend to kind of parse it out a little bit here, as we are doing in this hearing right now, talking specifically about disinformation. If this was going on in Russia right now, the conversation would probably be a little bit more overarching and incorporate a lot more of the traditional, what we would call old FSB [Federal Security Service] tactics as well. Again, we kind of parse it a bit, but they look at it much more holistically than we do.

Mr. LARSEN. So, not so much better or worse, but it is kind of based on how they have done it in the past; whereas, we have important limitations in place, based in the written Constitution, as a for instance, that say we can do certain things and we cannot absolutely do other things. That is just one example.

Mr. SULLIVAN. Sure. I will say this: in the United States, okay, we are not going to fabricate or alter data and release it publicly. The Russians would have no problem doing that, and do do that quite often.

Mr. LARSEN. Yes. Thank you, Mr. Chair.

Mr. GALLEGO. Thank you, Mr. Larsen.

If there are no other questions, we are going to adjourn for 15 minutes and move to our classified briefing in Rayburn 2212. Thank you.

[Whereupon, at 11:59 a.m., the subcommittee proceeded in closed session.]

A P P E N D I X

MARCH 16, 2021

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

MARCH 16, 2021

Opening Statement
Chairman Ruben Gallego
Subcommittee on Intelligence and Special Operations - Hearing
Disinformation in the Gray Zone: Opportunities, Limitations, and Challenges
March 16, 2021 – 11:00 AM – Rayburn 2118

Good morning.

I call to order this first hearing of the Intelligence and Special Operations Subcommittee on "Disinformation in the Gray Zone: Opportunities, Limitations, and Challenges."

We are seeing unprecedented threats to our democracy and a disturbing rise of authoritarian actors. Anti-democratic forces have capitalized on the rapidly evolving information environment to spread disinformation and misinformation, and exploit fissures in our society. The only way to reverse these trends is through a whole-of-society approach, working with partners and allies who share our values.

After two decades of war, fighting terrorists in Afghanistan, Iraq, and elsewhere around the Middle East and Africa, we have discovered an even greater threat inside the wire. Gone are the days when we could solely rely on the armed forces to fight our wars far beyond our borders. The threats and attacks are now here. On American soil. At home.

The 2018 National Defense Strategy stated that "the Homeland is no longer a sanctuary." Our adversaries' use of information and technology has proven that out. They craft and feed misinformation to our news outlets and social media – about the safety of vaccines, the efficacy of our institutions, and the depth of our differences – and then they weaponize our own reactions to that misinformation.

So, we have a problem. So much so that last year nine – 9! – combatant commanders co-signed a letter to the Director of National Intelligence requesting immediate help to combat the pervasive and damaging influence by China and Russia. I want to hear what we are doing to help our commanders. How are we making sure that information about the malign activities of Russia and China is not overclassified?

How are you synchronizing with the State Department, and with partners and allies, to combat these threats?

Information operations is one way that the United States can protect itself and its partners against dis- and mis-information efforts by China and Russia. But we should aspire for cohesion and breadth. We must develop a comprehensive influence strategy to truly protect our borders, our allies, and our interests.

In that context, I look forward to hearing from our witnesses about the Department's efforts to support and build that whole-of-government construct.

I want to introduce the three witnesses who'll tell us about that:

- Mr. Christopher Maier, Acting Assistant Secretary of Defense for Special Operations and Low Intensity Conflict,

- Mr. Neill Tipton, Director of Defense Intelligence, Collections and Special Programs, and
- Mr. James Sullivan, Defense Intelligence Officer

Following this discussion, we will continue in a closed, classified session.

UNCLASSIFIED

Joint STATEMENT FOR THE RECORD of
Mr. Christopher Maier, Acting Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict,
Mr. Neill Tipton, Director of Defense Intelligence (Collections and Special Programs), and
Mr. James Sullivan, Defense Intelligence Officer for Cyber, Defense Intelligence Agency
before the
HOUSE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON INTELLIGENCE AND SPECIAL OPERATIONS
on
"DISINFORMATION IN THE GRAY ZONE: OPPORTUNITIES, LIMITATIONS, CHALLENGES"

March 16, 2021

(U) Chairman Gallego, Ranking Member Kelly, and distinguished committee members, it is an honor to be with you today.

(U) We are here today to discuss the impact of "disinformation in the gray zone" and the Department of Defense (DoD) efforts to maintain the operational advantage in this evolving threat environment.

(U) The DoD understands "disinformation" to consist of the deliberate dissemination of false information with the intent to deceive. Examples include planting false news stories in the media, false narratives in social media, and tampering with private and/or classified communications before their widespread release. Disinformation is also closely related to misinformation, which can be defined as the unintentional dissemination of false information, for example, internet trolls who spread unfounded conspiracy theories or web hoaxes through social media, believing them to be true. "Disinformation" and "misinformation" both exploit false information. Effective false information is usually crafted from a kernel of truth, deliberatively manipulated with false information or selective omission of true context. The deliberate employment of mis- and disinformation can be considered in the execution of propaganda. Propaganda is the

UNCLASSIFIED

dissemination of an idea or narrative that is intended to influence. It may be misleading or true. An actor or government communicating its intent, policies, and values through speeches, press releases, and other public means can be considered propaganda.

(U) Adversary use of disinformation, misinformation, and propaganda poses one of today's greatest challenges to the United States, not just to DoD. Russia and China, as well as non-state actors, understand that in today's information environment they have real-time access to a global audience. With first-mover advantage and by flooding the information environment with deliberately manipulated information, i.e., mostly truthful with carefully crafted deceptive elements, these actors can gain leverage to threaten our interests.

(U) Russia sees the information sphere as a key domain for modern military conflict. Russia has prioritized the development of forces and means for information confrontation in a holistic concept for ensuring information superiority since at least the 1920s. Russia wages this struggle for information dominance during peacetime and armed conflict with equal intensity using combined electronic and kinetic means and methods through information-technical, information-psychological, and active measures. The Russian Government claims NATO countries, led by the United States, have created a powerful information operations (IO) system and are expanding and improving it.

(U) Russia sees the Information Domain differently than the United States and its allies and partners. Russian publications and actions indicate its government maintains a holistic concept of "information confrontation" ("informatsionnoye protivoborstvo"). Specifically, "information confrontation" seeks to dominate the Information Domain through a combination of what it defines as information-technical effects -- or means that seek to manipulate networks, computers and data -- and information-psychological effects all intended to target people or a population to influence behavior or opinions. We are increasingly seeing the integrated use of cyber-enabled psychological actions, distributed denial of service attacks, propaganda disseminated through social media and bots, strategic deception and disinformation, and electromagnetic warfare to achieve strategic goals.

(U) China seeks to influence domestic, foreign, and multilateral political establishments and public opinion to accept China's narratives and to remove obstacles that prevent China from attaining its goals, including the sustainment of the Communist Party regime. The People's Liberation Army (PLA) has developed the concept of "Three Warfares" – public opinion, legal, and psychological warfare -- as key components of its psychological-cognitive warfare efforts. These efforts are designed to demoralize adversaries and to influence foreign and domestic public opinions.

(U) Similar to Russia, China also takes a broad approach including the establishment of a state-directed global media network, overt and covert ties to Mandarin-language media in third countries, and the employment of cyber techniques. China views the cyber domain in particular as an ideal platform for strategic influence and deception and disinformation operations. The PLA likely seeks to use digital influence activities to support its overall "Three Warfares" concept and to undermine an adversary's social cohesion, economy, morale, and governance. These operations are conducted with equal intensity in peacetime and during armed conflict. The PLA goals for social media influence activities fall into broad categories: promote a narrative favorable to China, undermine adversary resolve and social cohesion, shape foreign governments' policies in favor of China's core interests

(U) Although we are here today to discuss various DoD efforts, we recognize that we do not have a monopoly on U.S. Government capabilities to combat disinformation, nor should we; the DoD is one part of a whole-of-government approach to this challenge, and other civilian departments and agencies have critical roles and responsibilities, which demand close interagency coordination and clear authorities. Disinformation contributes to an environment in which consumers of information trust no one. The United States and our allies and partners must continue to counter disinformation by exposing the lies and their sources, and providing factual information from trusted transparent sources. Coordinated interagency effects can complement the efforts of each department or agency to defend the nation against disinformation and to reach and engage global audiences.

(U) As we strive to leverage DoD's information operations capabilities in competition with malign actors, we first acknowledge – as reiterated in the recently published Interim National Security Strategic Guidance – that we will actively support elevating diplomacy as our tool of first resort. DoD will directly support and coordinate with the Department of State's Public Affairs and Public Diplomacy teams and the Global Engagement Center, as well as complement the U.S. Agency for Global Media operations.

(U) In addition, DoD will address the tasks required in Section 1631 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2020 to improve integration of policy, strategy, planning, resource management, operational considerations, personnel, and technology development across all the elements of information operations of DoD. The Secretary has designated a Principal Information Operations Advisor (PIOA) and will build a cross-functional team to assist in the accomplishment of the POIA's primary responsibilities. We have initiated the required Information Operations posture review, and that includes reviewing how the DoD is organized and is evolving to ensure we successfully execute operations in the information environment. We will keep the committee regularly informed on our progress.

(U) Within DoD, we view our efforts to combat disinformation, misinformation, and propaganda in four broad lines of effort all supported by a foundation of intelligence support, interagency collaboration, and partnerships: 1) countering propaganda by adversaries, 2) force protection, 3) countering disinformation and strategic deception abroad by adversaries; and 4) deterring and disrupting adversarial malign influence capabilities.

(U) Countering Propaganda

(U) Propaganda, especially with a capable sponsor spreading it to susceptible audiences, can often drown out truthful information and create barriers to fact-based messaging. Within DoD, Public Affairs is the lead for countering propaganda by adversaries that impacts U.S. military objectives and keeping domestic and foreign audiences informed of adversarial efforts to manipulate behavior in this domain. Other DoD capabilities support Public Affairs' efforts to lead proactively with truthful, verifiable, fact-based messaging. DoD efforts to engage foreign

audiences overseas support the leading U.S. Government role played by the Department of State to inform and influence foreign audiences.

(U) Force Protection

(U) Our Soldiers, Sailors, Marines, Airmen, Guardians, civilians, and their families are part of the American public directly targeted by malign actors' disinformation, misinformation, and propaganda. DoD views this as a critical force protection issue. The Services are proactively leading efforts to enable resilience against these threats. Enabling the force to recognize deceptive information tactics by adversarial information operations, developing digital literacy, and employing critical thinking skills are a few key initiatives within this line of effort.

(U) Countering Disinformation Abroad

(U) DoD also possesses operational and informational capabilities, such as Military Information Support Operations (MISO), to generate narratives to compete against disinformation efforts directed at foreign audiences. These DoD capabilities can amplify as well as act in a complementary manner to inform audiences that cannot be reached through traditional communication channels. We will take a comprehensive and deliberate approach in consultation with the Department of State, taking into account the agility, capability, and capacity to connect with audiences globally in real time to build communications that foreign audiences trust. Knowledge and trust by foreign audiences will reduce and even suppress the impact of malign influence activities. DoD will continue to review ongoing work within the Department of State and seek ways to increase collaboration with the Department of State to optimize such efforts against these evolving threats and challenges in the information environment.

(U) Deterring and Disrupting Adversarial Malign Influence Capabilities

DoD's greatest strength lies in its capability to align narratives, actions in the land, sea, air, cyber, and space domains, and information-related capabilities against key weaknesses in the adversaries' information environment. Additionally, DoD has the knowledge, skills, and

infrastructure to enable partners, allies, proxies, and surrogates to compete with malign actions as peer competitors in the information environment. DoD's ability to execute Dynamic Force Employment enables diplomatic actions to deter malign behaviors by adversaries, incentivize their cooperation, or, when necessary, compel action.

(U) In addition to DoD's ability to match words with deeds, we also complement these actions with ongoing efforts to defend forward, which actively detects, assesses, and, when directed, disrupts adversaries' disinformation, misinformation and propaganda.

(U) Pursuant to section 1239 of the NDAA for FY 2020, we also are working to develop the comprehensive strategy to counter the threat of malign influence by the People's Republic of China and the Russian Federation. Those efforts are developed in concert with interagency partners, coordinated by the National Security Council staff.

(U) Partnerships and Intelligence Support

(U) Underpinning all these efforts is a strong commitment to a whole-of-government partnership and decision cycle that constantly assesses the effects of misinformation and propaganda, and seeks to attribute those efforts to the responsible parties. This requires active cooperation across responsible departments and agencies as well as direct support from the Intelligence Community. DoD leverages its information capabilities to gain and maintain the information advantage and integrates with the tools of other departments and agencies as part of a broader and more comprehensive approach. Our international allies and partners also bring reinforcing and often unique capabilities to countering adversaries' malign efforts; their capabilities will be integrated into our planning efforts as well.

(U) The recently signed Defense Intelligence Strategy (DIS) prioritizes the threat from China and Russia. The strategy calls out the specific action to prioritize intelligence support to strategic competition and influence efforts. The Defense Intelligence Enterprise (DIE) will help advance U.S. influence and counter coercive campaigns via intelligence support to sensitive and special activities, influence, deception, and operations in the information environment. We would like to

highlight for the committee three specific examples of ongoing actions that the Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)) is supporting by leveraging its roles within DoD and the greater Intelligence Community: 1) Intelligence support to Irregular Warfare, 2) Intelligence support to Operations in the Information Environment (OIE), and 3) Intelligence dissemination to support Combatant Command Messaging.

(U) Intelligence Support to Irregular Warfare

(U) In support of the Irregular Warfare (IW) Annex to the 2018 National Defense Strategy, OUSD(I&S), in partnership with the Joint Staff J2, supports specific lines of effort to enable DoD to improve understanding in a Multi-Domain Environment. The several lines of efforts focus on identifying Indicators and Warning, integrating collection, leveraging big data, reinforcing intelligence-sharing best practices, and assessing policies and processes to support these efforts.

(U) Intelligence Support to OIE

(U) In December 2018, the DoD Information Operations Executive Steering Group (IO ESG) directed the formation of a working group to optimize intelligence support to OIE. In April 2019, OUSD(I&S) chartered the Defense Intelligence Support to Operations in the Information Environment Working Group (DISOIE-WG), whose members include representatives from across OUSD(I&S), the Office of the Under Secretary of Defense for Policy, the Office of the Under Secretary of Defense for Acquisition and Sustainment, the Combat Support Agencies, the Defense Counterintelligence and Security Agency, the Joint Staff, the Joint Information Operations Warfare Center, and Intelligence representatives from each of the Services and U.S. Special Operations Command. The DISOIE-WG was created to improve intelligence integration and support to OIE by examining how collection, analysis, and prioritization of intelligence activities and capabilities can be optimized through policy, oversight, governance, enablement, and advocacy.

(U) In 2020, the DISOIE-WG proposed a new effort to focus National Intelligence Community collection efforts on assisting the conduct of influence-related activities against key adversaries. That work is still ongoing.[1]

(U) Currently, the DISOIE-WG is focused on drafting and staffing a new DoD Instruction for intelligence support to OIE activities; acting upon recommendations in a 2019 Joint Review Oversight Council Memorandum on OIE to address the Joint Staff capabilities based assessment; directing the DIE to prioritize resources for intelligence support to OIE in the next published Consolidated Intelligence Guidance; and engaging and participating in the National Intelligence focus groups to help drive key concepts related to OIE activities.

(U) Combatant Command Support

(U) Another line of effort for which DoD is providing intelligence support to OIE has been the joint DoD-Director of National Intelligence (DNI) response to the intelligence demands from the Combatant Commands. In January 2020, nine Combatant Commanders signed a memorandum, known colloquially as the "36-star memo," asking for increased support from the Intelligence Community for messaging and countering disinformation operations as part of great power competition. In response, the USD(I&S) and DNI partnered in an ongoing effort to streamline processes for downgrading, declassifying, and disclosing intelligence in support of OIE. DoD will look to complete the current efforts in response to the "36-star memo" by September 2021, while continuing with follow-on initiatives to increase the use of Open-Source intelligence and to determine policy and resourcing strategies to provide the most effective intelligence support to OIE going forward. Additionally, DoD is working to improve its training of intelligence personnel and to optimize its tradecraft as appropriate to support OIE.

(U) In conclusion, DoD recognizes the threat of disinformation, misinformation, and propaganda; we continue to invest our capability to improve employment of information operations and other tools to mitigate and defeat our adversaries' disinformation efforts. We will

[1] (U) COVID-19 impacted the Working Group's 2020 objectives.

continue to improve our speed, agility, efficiency, teamwork and most importantly – effectiveness.

Christopher P. Maier
Acting Assistant Secretary of Defense for
Special Operations/Low-Intensity Conflict

Christopher P. Maier is the Acting Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict. Among his responsibilities are all special operations, irregular warfare, counterterrorism, and information operations policy issues and the oversight of special operations peculiar administrative matters, on behalf of the Secretary.

He previously led the Department of Defense's Defeat-ISIS Task Force from its inception until disestablishment, charged with policy and strategy development, international negotiations, oversight, authorities review, and national-level interagency implementation of the Department's role in the U.S. Government's campaign to achieve an enduring defeat of ISIS. In this role, he also directed the Secretary of Defense's leadership of the Defense Ministry components of the 80+ international members of the Defeat-ISIS Coalition.

From July 2015 to September 2017, Mr. Maier served as the Deputy Assistant Secretary of Defense for Special Operations and Combating Terrorism. In this role, Mr. Maier led the Department's policies, plans, authorities and resources related to special operations and irregular warfare, with special emphasis on counterterrorism, counterinsurgency, unconventional warfare, information operations and sensitive special operations.

Before moving to the Department of Defense, Mr. Maier held a number of positions at the National Counterterrorism Center (NCTC), including Senior Advisor to the Director, Chief of Strategic Assessments and Regional Planning, and Chief of Staff in the Directorate of Strategic Operational Planning.

From 2009 to 2013, Mr. Maier served on the National Security Council Staff as a director for counterterrorism. In addition to his government experience, Mr. Maier worked for over five years as a strategy and management consultant to a variety of commercial, government, and nonprofit organizations.

Originally from California, Mr. Maier earned degrees from the University of California, Berkeley and the Fletcher School of Law and Diplomacy at Tufts University. He is an officer in the Air National Guard.

Neill Tipton
Director for Defense Intelligence, Collection and Special Programs

Mr. Neill Tipton serves as Director for Defense Intelligence, Collection and Special Programs, Office of the Under Secretary of Defense for Intelligence.

Mr. Tipton has been with the Office of the Under Secretary of Defense for Intelligence since 2007. He has held a broad range of leadership positions for the office: Director, Clandestine Operations, Global Access, and Mission Integration and Director, GEOINT and SIGINT Support; Director, Information Sharing and Partnership Engagement and IPT Lead for Information Sharing and Collaboration for the SECDEF's ISR Task Force; Deputy Director, SIGINT and Cyber; and as OUSDI Senior Advisor for Technical Collection.

During his tenure with OUSDI, he also served on detail as Deputy Director, Defense Technology Integration Program Office and to the Office of the Director of National Intelligence, as the Chief of the Collection Integration Group.

Prior to OUSDI, Mr. Tipton worked for the National Geospatial-Intelligence Agency. While with NGA he held leadership positions principally focused on improving NGA's integration with other elements of the Intelligence Community and the DoD.

Mr. Tipton has more than 38 years of experience in the intelligence community, with extensive expertise in the management and conduct of SIGINT, MASINT, and GEOINT operations. His background includes a wide range of intelligence activities, including Army and joint operations, National intelligence operations at NSA and NGA, all-source analysis, and extensive oversight and policy activities.

Mr. Tipton retired from the US Army in 1999 after twenty years as a SIGINT specialist with assignments in Latin America, Germany, Korea, Operation Desert Storm, and multiple CONUS locations, including two tours at NSA.

Mr. James Sullivan
Defense Intelligence Officer for Cyber
Defense Intelligence Agency

Mr. Jim Sullivan became the Defense Intelligence Officer for Cyber in December 2019. In this role, Mr. Sullivan advises DIA leadership and other Department of Defense (DoD) and Intelligence Community (IC) officials on defense cyberspace-related topics of interest to the Department and policymakers. He helps ensure that cyberspace is normalized as a domain of warfare and that processes, roles, and responsibilities for intelligence support to cyberspace operations are well understood and executed among the constituent members of the Defense All-Source Analytic Enterprise (DIAAE), DoD, and the IC.

Mr. Sullivan was appointed to the senior ranks in October 2017, as the Senior Expert for Military Cyber Intelligence Operations, United States Cyber Command, Ft. Meade, Maryland. In this assignment, he was responsible for overseeing the all-source analytic effort at USCYBERCOM and integrating production and collection requirements across the Defense Intelligence Enterprise in support of military operations in cyberspace.

A native of New Jersey, Mr. Sullivan joined the Defense Intelligence Agency in 1996, after graduating from Montclair State University with majors in English and History. He received a Master of Arts in National Security and Strategic Studies from the U.S. Naval War College in 2005, and a Master of Science in National Security Strategy from the National War College in 2009.

Prior to his appointment at USCYBERCOM, Mr. Sullivan served in a number of positions within the analytic career field, including assignments on the Joint Staff, as a Deputy Defense Senior Representative to USCYBERCOM, Deputy National Agency Representative to NSA, Director, Civil-Military Integration Program in Afghanistan, and as a C4I analyst focused on Russia and China and as a C4I Subject Matter Expert in Operations ALLIED FORCE, ENDURING FREEDOM and IRAQI FREEDOM.

His awards include the National Intelligence Medal of Achievement, Joint Civilian Service Commendation Award, and NATO Medal.

○